

WHAT IS CLAIMED IS:

1. A shared library call method for a computer for executing an operating system which loads application programs and shared libraries in the same virtual space and manages a memory so as to make each application program have a specific virtual space, said method comprising the steps of:

hooking a call to a function in said shared library from said application program, the call being hooked by an injection shared library;

in response to hooking the call, calling a module stored in a kernel region of said memory; and

executing at least one process in accordance with information set in said called module, and thereafter calling the function in said shared library.

2. The shared library call method according to claim 1, wherein said module records a content of said hooked call to said shared library in said kernel region.

3. The shared library call method according to claim 2, wherein said module audits the content of said hooked call in accordance with a predetermined policy and determines whether the hooked call to said shared library is to be permitted or not.

4. The shared library call method according to claim 3, wherein a result of the determination of permission or not is recorded in said kernel region.

5. The shared library call method according to claim 4, wherein a region where said call content is recorded in said kernel region is prepared for each of a plurality of processors.

6. The shared library call method according to claim 5, wherein a control application is provided for acquiring said call content recorded in said kernel region.

7. The shared library call method according to claim 6, further comprising the steps of:

issuing a command of changing settings in said module from said control application;

storing said issued command in a predetermined region in said kernel region; and

changing the settings in accordance with the command stored in said predetermined region, the settings being changed by said module.

8. The shared library call method according to claim 7, further comprising the steps of:

issuing a command of setting said auditing policy from said control application;

storing said issued command in a predetermined region in said kernel region; and

setting said auditing policy in accordance with said command stored in said predetermined region, said auditing policy being set by said module.

9. A computer for executing an operating system which loads application programs and shared libraries

in the same virtual space and manages a memory so as to make each application program have a specific virtual space, comprising:

hooking means for hooking a call to a function in said shared library from said application program, the call being hooked by an injection shared library;

module calling means responsive to hooking of the call for calling a module stored in a kernel region of said memory; and

means for executing a predetermined process in accordance with information set in said module called by said module calling means, and calling the function in said shared library in accordance with a result of said process.

10. The computer according to claim 9, wherein said module stored in said kernel region includes a filter module, and said filter module records shared library call information and audits the shared library call.